EXHIBIT 10

NORTON ROSE FULBRIGHT

August 27, 2018

FRE 408 Communication

Via Email: wramey@rameyfirm.com
and First Class Mail

William P. Ramey, III
Ramey & Schwaller, LLP
5020 Montrose Blvd., Suite 750
Houston, Texas 77006

Norton Rose Fulbright US LLP
2200 Ross Avenue, Suite 3600
Dallas, Texas 75201-7932
United States

Robert Greeson
Partner
Direct line +1 214 855 7430
robert.greeson@nortonrosefulbright.com

Tel +1 214 855 8000
Fax +1 214 855 8200
nortonrosefulbright.com

Re: WPEM, LLC v. SOTI Inc.

Bill:

As I have previously stated, the technology WPEM refers to as the "SOTI MobiControl," i.e., the "Accused Technology," was in use and publicly available before the priority date of U.S. Patent No. 9,148,762 (the "'762 Patent"). Specifically, Version 10 of the SOTI MobiControl, which included all Speed Lockdown functionality found in the current version of the SOTI MobilControl, was in use and publicly available before the priority date of the '762 Patent. This is clearly demonstrated by publicly-available information, some of which is provided herewith. As I have further explained, the only differences between Version 10 of the SOTI MobiControl and the current version of same are limited to very minor changes (i.e., patches and the like). Necessarily, then, to the extent WPEM alleges that the SOTI MobiControl includes the features of the claims of the '762 Patent, the SOTI MobiControl invalidates such claims.

WPEM's Complaint relies on portions of the MobiControl Help PDF to allege infringement of each claim of the '762 Patent. As we have discussed, the accused functionality of MobiControl (e.g., Speed Lockdown) has not substantively changed since Version 10, which was publicly released no later than January 7, 2013—four (4) months before the '762 Patent's priority date of May 9, 2013.

The following table lists each page of the MobiControl Help PDF cited in WPEM's Complaint as allegedly practicing each element of the '762 Patent, along with corresponding portions of the Version 10 manual *that demonstrate the same functionality*:

MOBICONTROL HELP PDF PAGES CITED IN WPEM'S COMPLAINT	VERSION 10 HELP MANUAL SHOWING SAME FUNCTIONALITY
685-687	01_MobiControl v10 speed lockdown.pdf
110	02_MobiControl v10 location services.pdf
674	03_MobiControl v10 application run control.pdf

MOBICONTROL HELP PDF PAGES CITED IN WPEM'S COMPLAINT	VERSION 10 HELP MANUAL SHOWING SAME FUNCTIONALITY
693	04_MobiControl v10 custom data variables.pdf
698	05_MobiControl v10 phone call policy.pdf
341	06_MobiControl v10 device relocation rules.pdf
122	07_MobiControl v10 manage geofence.pdf
696	08_MobiControl v10 device feature control.pdf
1284	09_MobiControl v10 web console.pdf

For your reference, the documents referenced in the foregoing table that describe the functionality of Version 10 of the MobiControl are attached hereto. The following documents, which further clarify this point, are also attached:

- MobiControl release notes demonstrating that Speed Lockdown was introduced in Version 10.0 Build 9329, *January 7, 2013* (10_2013-01-07_MobiControl Release Notes - SOTI.PDF); and
- Wayback machine capture *demonstrating MobiControl Version 10 was publicly available at least as early as January 16, 2013* (11_2013-01-16_V10_SOTI MobiControl - Mobile Device Management (MDM).pdf)

In view of the foregoing, from any reasonable view point, the Accused Technology predates the '762 Patent. As you know, FRCP 11 imposes an obligation on an attorney to (1) conduct a reasonable pre-suit investigation before alleging infringement; and (2) evaluate the reasonableness of claims of infringement in view of information discovered during litigation.

Therefore, under FRCP 11, (1) SOTI should not have been sued to begin with, and (2) WPEM must dismiss its claims of infringement. Refusing to do so strongly supports a claim SOTI may bring for sanctions under FRCP 11, attorneys' fees under 35 U.S.C. 285, and/or costs under 28 U.S.C. 1927.

Please let me know if you want to discuss by phone. Otherwise, I look forward to your response.

Very truly yours,

Robert Greeson

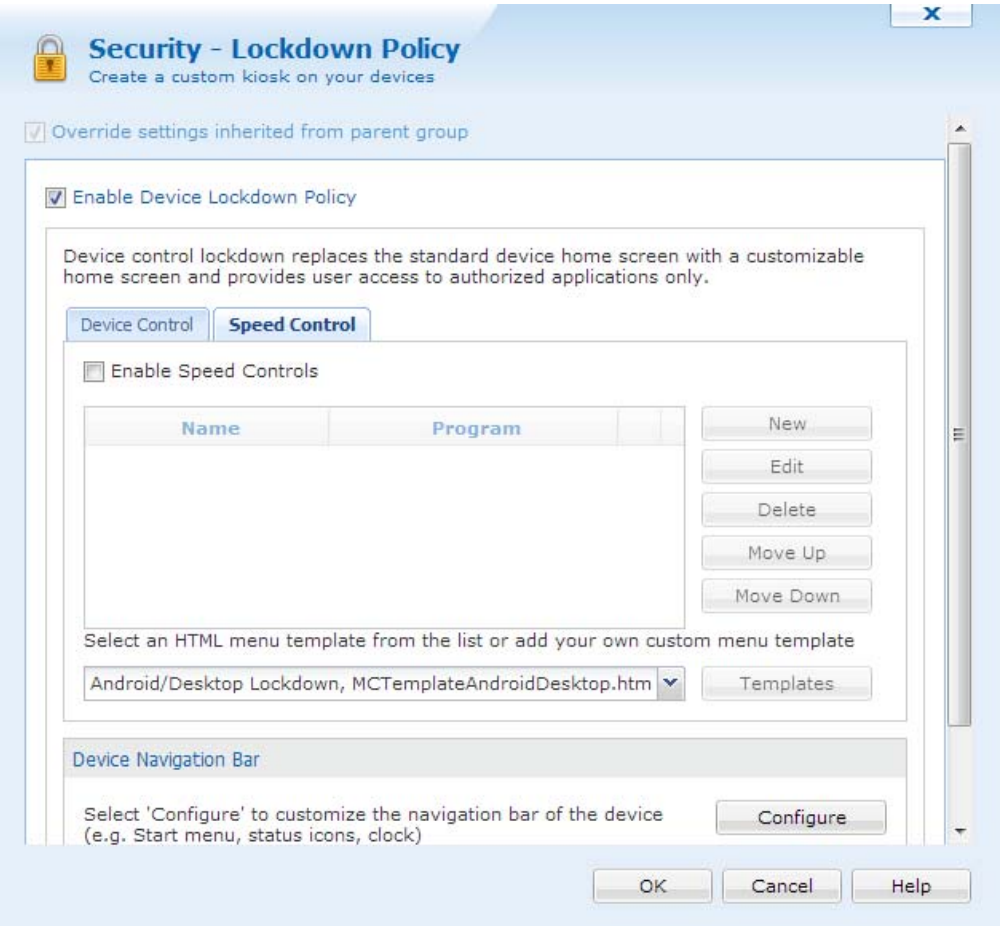
RLG

Attachments:

01_MobiControl v10 speed lockdown.pdf
02_MobiControl v10 location services.pdf
03_MobiControl v10 application run control.pdf
04_MobiControl v10 custom data variables.pdf
05_MobiControl v10 phone call policy.pdf
06_MobiControl v10 device relocation rules.pdf
07_MobiControl v10 manage geofence.pdf
08_MobiControl v10 device feature control.pdf
09_MobiControl v10 web console.pdf
10_2013-01-07_MobiControl Release Notes - SOTI.PDF
11_2013-01-16_V10_SOTI MobiControl - Mobile Device Management (MDM).pdf

Windows Mobile Speed Lockdown

Device lockdown replaces the standard device home screen and Windows **Start** button with a customizable home screen. Users have access only to authorized applications and websites, and are prevented from accessing all other applications and device controls while on the road. This promotes greater safety by disabling distracting features on a mobile device while workers are on the road.



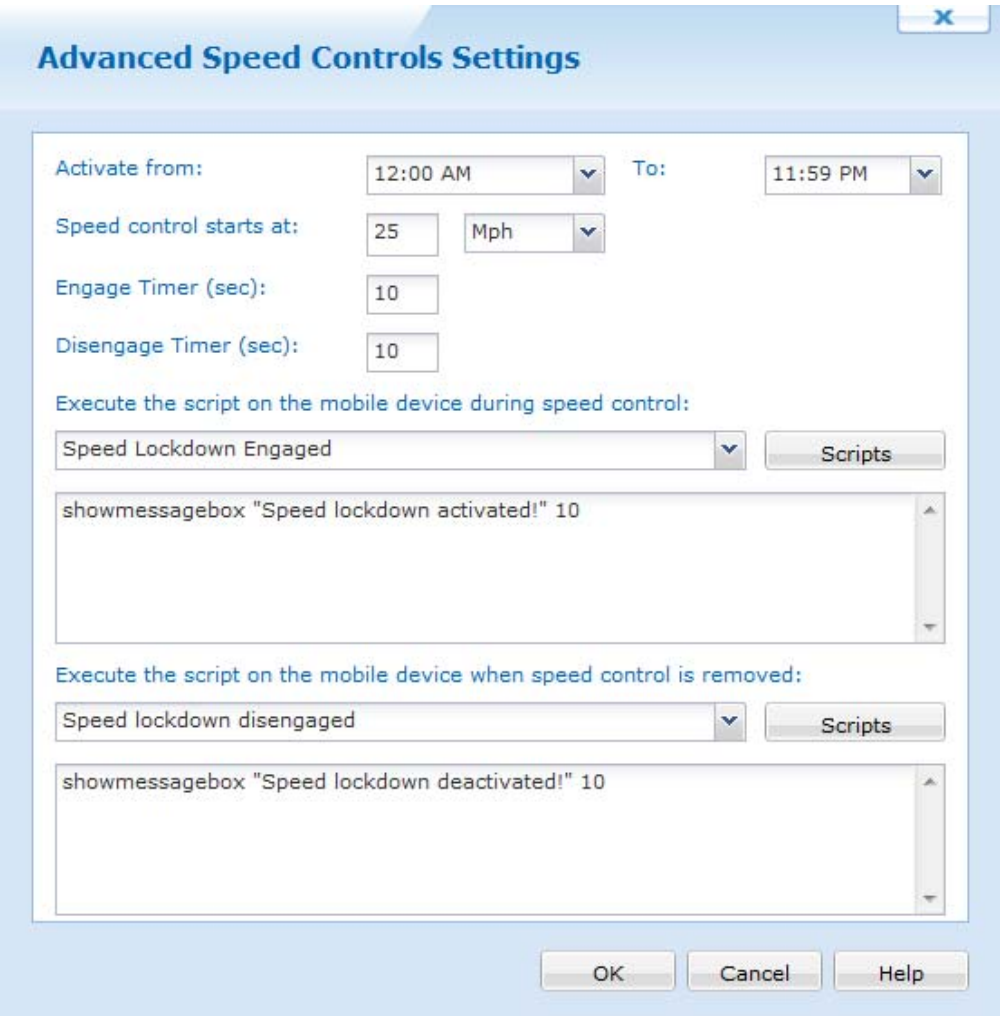
Lockdown Policy dialog box

For information on how to set up menu items and configuring lockdown templates, please click here.

Speed Lockdown triggers when the device is going a certain speed, as set in the Advanced settings. The speed of the device is determined by utilizing the device's GPS unit. Using the device's GPS unit, MobiControl periodically checks the location of the device along with the time. It will then check again and determine the distance between the two points and calculate the device's speed.

Since there are times where there could be traffic, or stop lights, having the speed lockdown disengage and re-engage constantly will cause distraction to a driver. Because of this, the speed lockdown has engage and disengage functionalities. These and other settings can be configured by clicking Advanced.

 Contact us



Advanced Speed Control Settings

Below are brief descriptions of each feature in the Advanced Speed Control settings.

Field	Description
Activate From, to	Here we can set when the speed control should activate. We can set it for the whole day or even 15 minutes.
Speed Control starts at	This is where we decide what speed the device should be travelling before the engage timer starts counting. We can change the speed measurement to either Mph or Km/h.

Field	Description
Engage Timer	The amount of time the device should stay on or above the speed control before the lockdown activates.
Disengage Timer	The amount of time the device stays below the specified speed control before disengaging.
Execute script on the mobile device during speed control	When the speed control lockdown is activated, send this script to the device.
Execute script on the mobile when speed control is removed	When the speed control lockdown is deactivated, send this script to the device.

Using the above screen shot, the speed lockdown is activated the whole day, should engage when the device is travelling at 25 Mph or higher for at least 10 seconds. If it falls below the specified speed, wait 10 seconds before disengaging the speed control. When the speed control is activated, send a message box to the device, and when the speed control is removed, send another script.

Location Services

MobiControl's Location Services provides the ability to locate and track mobile devices that are equipped with a GPS receiver that is internal or external to the unit. In order to locate a device, the GPS must be enabled and correctly configured on your device. The GPS determines the current location based on its position relative to orbiting satellites. In order for this to happen, the device requires a clear view of the sky. Determining location may not be possible if the device is inside buildings or has an obstructed view of the sky.

You can activate Location Services for a device in MobiControl by right- clicking on a device and selecting the **Location Services** option from the menu. The first time you select an option from the Location Services menu for a device, it will automatically use the next available license. If there are no more licenses available, you will be notified to contact SOTI for information on acquiring additional licenses for Location Services.

Please See "Contact Us" page to contact us for more details on acquiring additional licensing.

To learn more about Location Services, read about its features on the following pages:

Locate Devices page to pin-point the exact location of the mobile device anywhere in the world.

Track Devices page to follow the location of the device in real time.

Location History page to plot where the device has travelled over a certain duration of time.

Go to Location page to locate and zoom the map to a specific address or landmark

Get Directions page to generate turn by turn directions and send them to the device.

Address Lookup page to find the physical address of a location on the map.

Using the Manage Geofences page to View, Edit and Delete the Geofences you have created.

NOTES:

- When using Location Services in MobiControl to track devices, Internet Explorer 7 or higher is required.
- The Current Format for Regional and Language Options on your PC MUST be compatible with Bing Maps. Click here for a list of supported Bing Map control settings.

Contact us

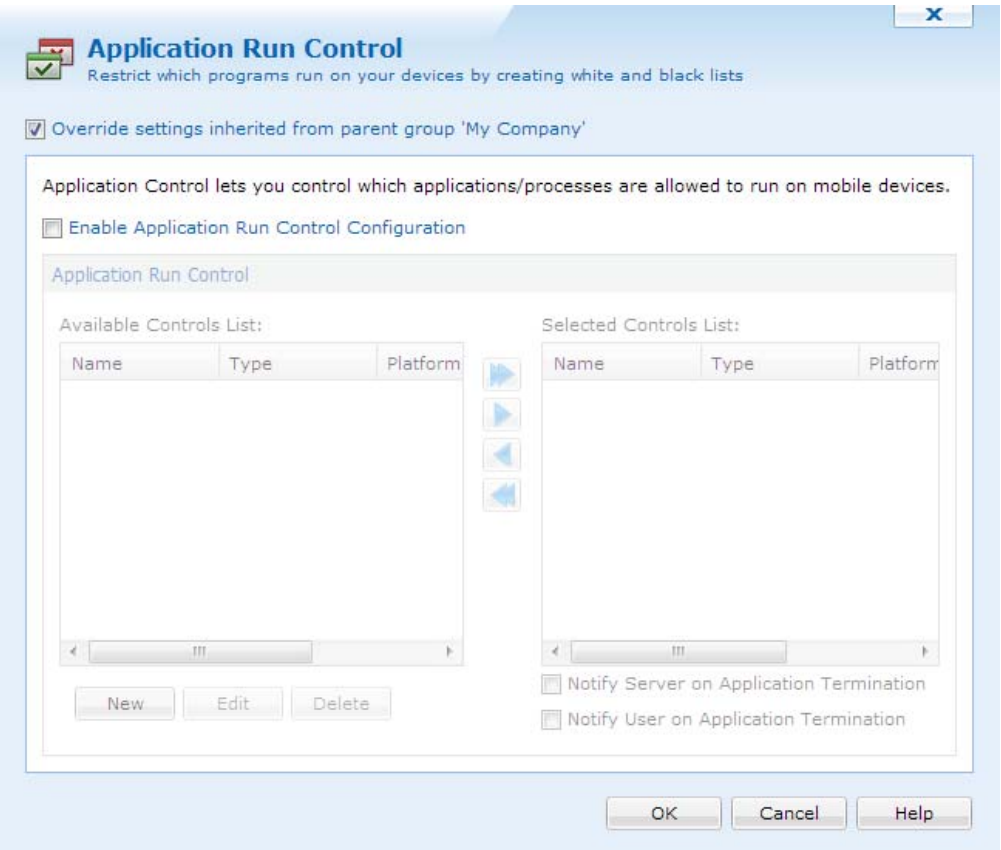
Windows Mobile Application Run Control

The easy availability of applications—games, consumer-oriented utilities and third party tools—for mobile devices results in end users installing and running unauthorized personal programs and recreational software on devices meant for business use. In addition to contributing to memory and battery life overhead, this situation also contributes to productivity losses. The installation of unauthorized and unapproved non-business applications contributes to a significantly higher volume of support calls, increasing the IT help desk's support burden. Most critically, it is imperative for security-conscious users to control and restrict the unauthorized installation of personal applications to ensure compliance with strict mobile data protection requirements.

MobiControl's application run control features reduce the risk of leakage of sensitive data and complement the existing network security model by preventing the introduction of malware and viruses into the network through the mobile devices. Additionally, it also allows memory management on the mobile devices to free up resources taken up by unnecessary processes, and allowing for better device performance. MobiControl integrates tightly with the operating system to prevent restricted applications from running entirely on the mobile device, making it much more efficient than competing white list and black list solutions which use CPU and battery-consuming processes to monitor for and destroy restricted applications.

IMPORTANT:

Due to some limitations in CE6 and higher, the Application Run Control cannot be configured on these devices.



Application Run Control dialog box

For assistance with Override Settings Click Here.

Contact us

Application Run Control Modes

MobiControl provides two modes of operation for Application Run Control with two control list types:

1. The **black list**, or list of restricted applications, allows IT administrators to ensure that an application will not be allowed to execute on the device. The MobiControl Device Agent prevents any black-listed processes from executing on the device.

   NOTE:

   If an application is being run from the lockdown, and it is blacklisted on the device, the application will still run as the lockdown takes precedence over the blacklist.

2. The **white list**, or list of approved/allowed applications, limits what programs can be executed on the devices. Only the applications and processes included in the white list are allowed to execute on the device. This provides an added layer of security for organizations concerned about unknown processes and applications that may be introduced to the device—maybe without the end user being aware of it, as is frequently the case with viruses, spy ware and other malicious applications.

   IMPORTANT:

   If the white list is not set up correctly, you may end up blocking a potential system critical applications and cause the device to crash.

To enable application run control for a device or group of devices, select **Application Run Control Policy** from the MobiControl Security Center. (Please see the Windows Mobile Device Configuration page.)

Control List Creation Methods

IMPORTANT:

Whether you are creating a white list or a black list, the use of learning mode is strongly encouraged.

Configuration of application run control begins with the creation of an application control list. An application control list is simply a listing of the names of the executables files that correlate to the application you may wish to allow or disallow on the mobile device. For example, `pword.exe` corresponds to Microsoft Word for Windows Mobile, and `tmail.exe` corresponds to Microsoft messaging client for Windows Mobile. The categorization of the application control list, either as a white list or a black list, determines whether the specified programs will be allowed or disallowed.

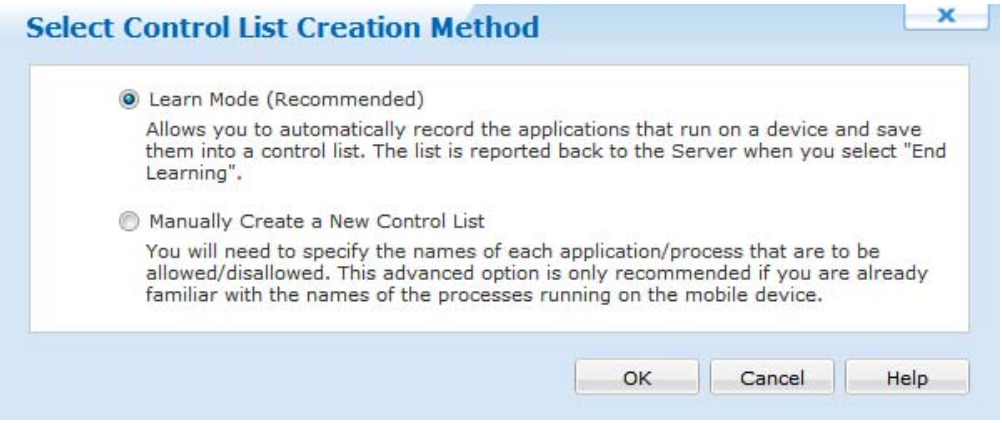
Application control lists may be specified manually or they can be auto-generated using learning mode.

Learning Mode

Learning mode can only be enabled or disabled on a device that is **online**. If you right-click on a device group or an offline device, you will receive an error message if you try to enable learning mode.

Learning mode allows you to quickly and easily capture the names of all the executable processes that might be relevant to the everyday use of the device by the end user. Once generated, you may edit the list that was created. One device

can be used to capture the applications that are commonly used. A control list can then be applied to a larger set of devices, for instance by applying the control list at a group level.

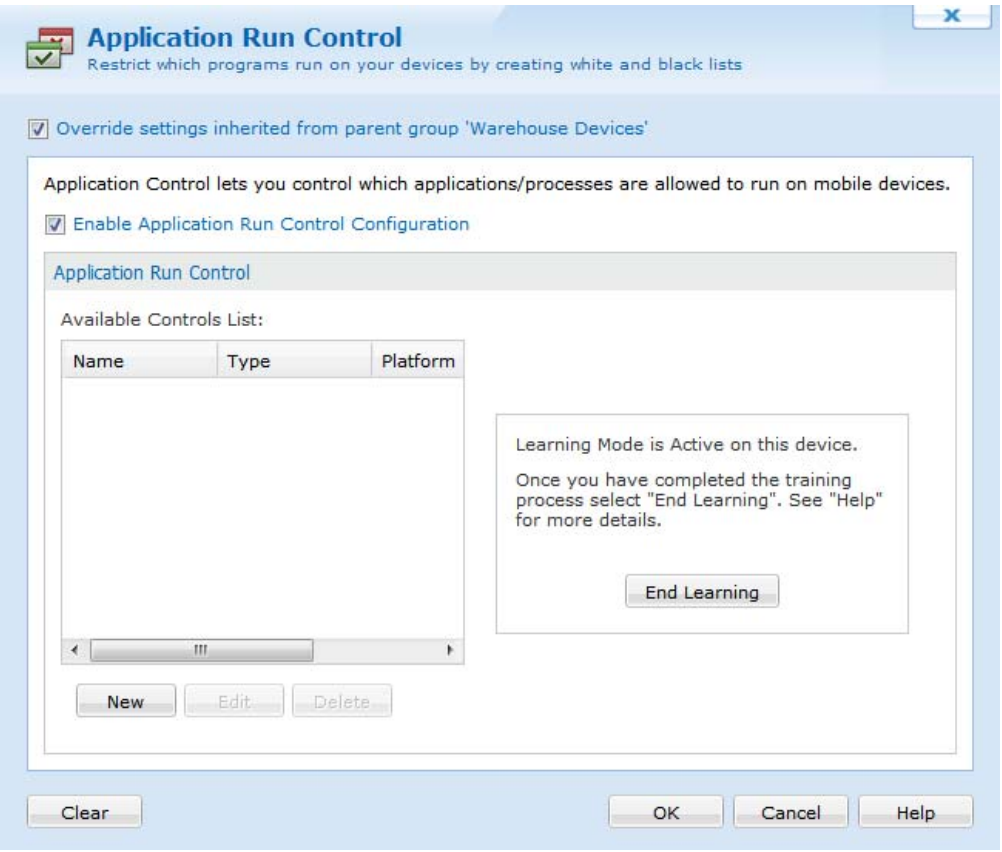


Select Control List Creation Method dialog box

Enable learning mode by selecting the **New** button in the **Application Run Control** dialog box, and then choosing **Learning Mode** in the **Select List Creation Method** dialog box.

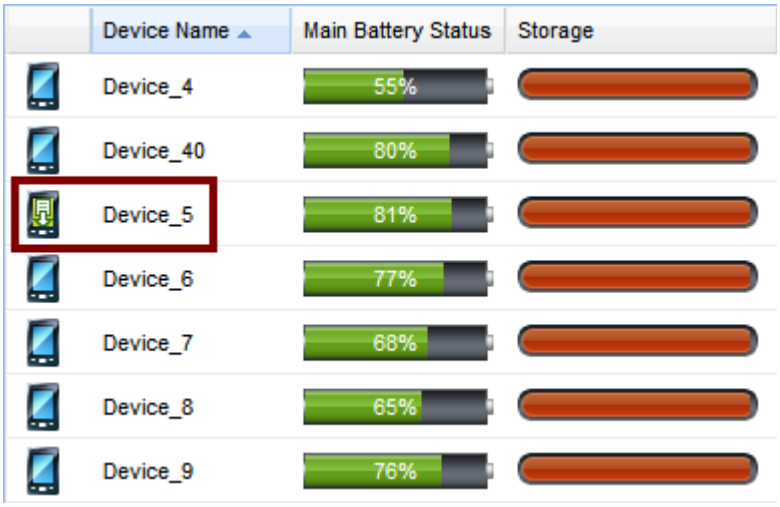
Once you have enabled learning mode, begin using the device. If you wish to develop a white list, run all the applications that the typical end user will need (i.e. Microsoft Messaging, Microsoft Word, Calendar, Contacts). Go through normal, everyday situations like making and receiving a phone call, soft-resetting the device, etc. Use the device with learning mode enabled for as long as it takes you to ensure that all the applications that your user will need to execute have been launched at some point. (You can run it for an hour, a day, a week,…)

Once you are satisfied that you have fully trained the device's application run control, click the **End Learning** button.

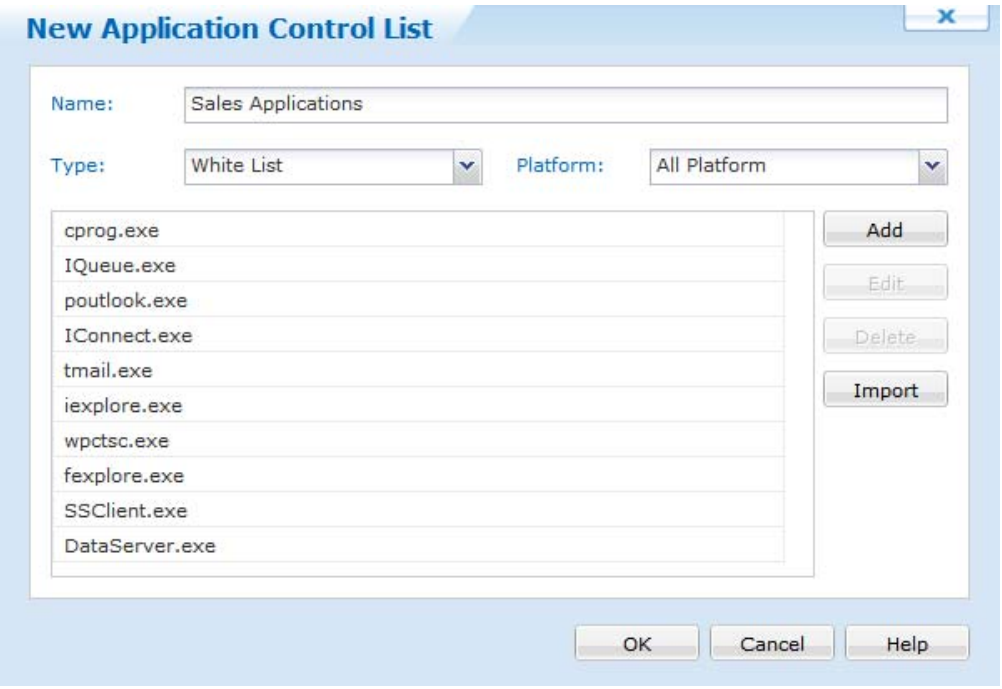


Application Run Control Learning Mode dialog box

While the device is in learning mode, a red **L** icon will appear on the device until learning mode has ended.



The list of "learned" applications will be presented to in a dialog box that allows you to edit the list. For example, you may wish to delete an application that was mistakenly executed during the learning. Before saving the control list, you must name it.

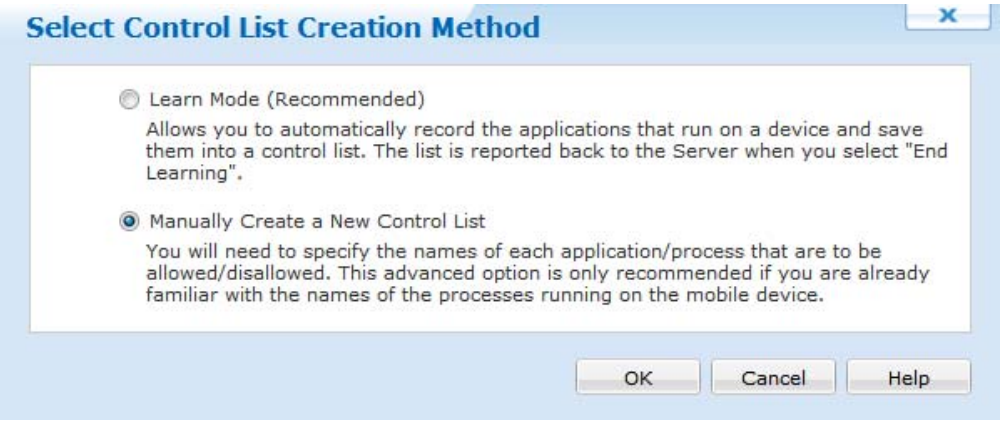


Application Run Control Learning Mode list

Now the application run control list has been created, you may assign it to various devices and groups.

If you wish to develop a black list using the Learning Mode, run all the applications that you do not want your user to be able to access (i.e. Solitaire, Bubble Breaker, Internet Explorer, etc.) Once you are satisfied that you have executed all the applications that are to be banned, click **End Learning.** Since learning mode lists all the processes that were found to be running, it is important that you go through and remove from the blacklist those application that are not to be disallowed.

Manual Mode



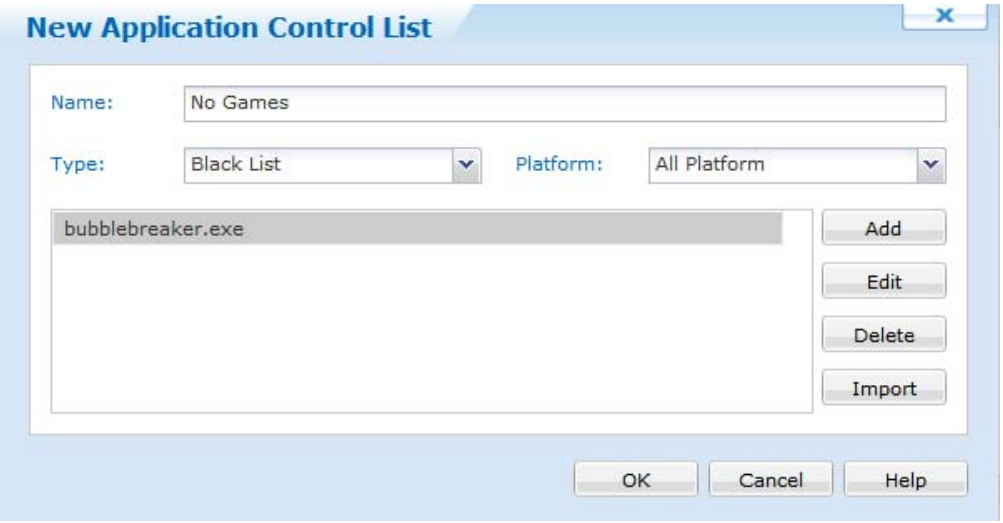
Select Control List Creation Method dialog box

Manual list creation is provided for the expert device administrator who already knows exactly which executables are to be put on the white list or black list. This advanced feature is only recommended if you have already used learning mode and are aware of the names of the executables that need to be allowed for correct device operation, and those that you wish to restrict.

Contact us

You can manually create a new application control list by clicking the **New** button in the **Application Run Control** dialog box, and then choosing the **Manually Create a New Control List** option in the **Select Control List Creation Method** dialog box. The **New Application Control List** dialog pops up, allowing you to specify the application that you want to add to the list, and the platform for which this entry would be valid. This allows you to restrict applications on a device running a specific operating system (e.g. Windows Mobile 5), if you have a mix of devices with different operating systems in the same group.

Once created, the list may be applied to one or more devices or groups.



Creating a black list in manual mode

IMPORTANT:

Application run control can adversely impact the operation of the mobile device if configured incorrectly. After you have developed a control list, apply it to one or two select devices for extended field testing before expanding it to the general deployment. As a general rule, if you don't know what the executable does (e.g. `somestrangename.exe`), allow it to run instead of blocking it as it might be critical for the device's proper operation.

Modifying or Deleting a Control List

An application control list can be edited whether it is currently in use or not, but its type (white list or black list) cannot be changed once created.

An application control list can only be deleted if it is currently not selected for any devices or device groups. A control list that is listed in the **Selected** field is considered in-use, even if the application run control is disabled for the given group or device.

NOTE:

If you edit an application control list that is shared among device groups that are not subgroups of the group you are configuring, the changes will not be propagated to the other devices. The modified control list will only affect devices belonging to the group being configured or its subgroups.

 Contact us

Application Run Control Event Notification

Every time MobiControl's application run control feature blocks or terminates an application that is not allowed to run by the security policy in effect, it can notify the server or the user if the appropriate options are selected.

The following two options are available:

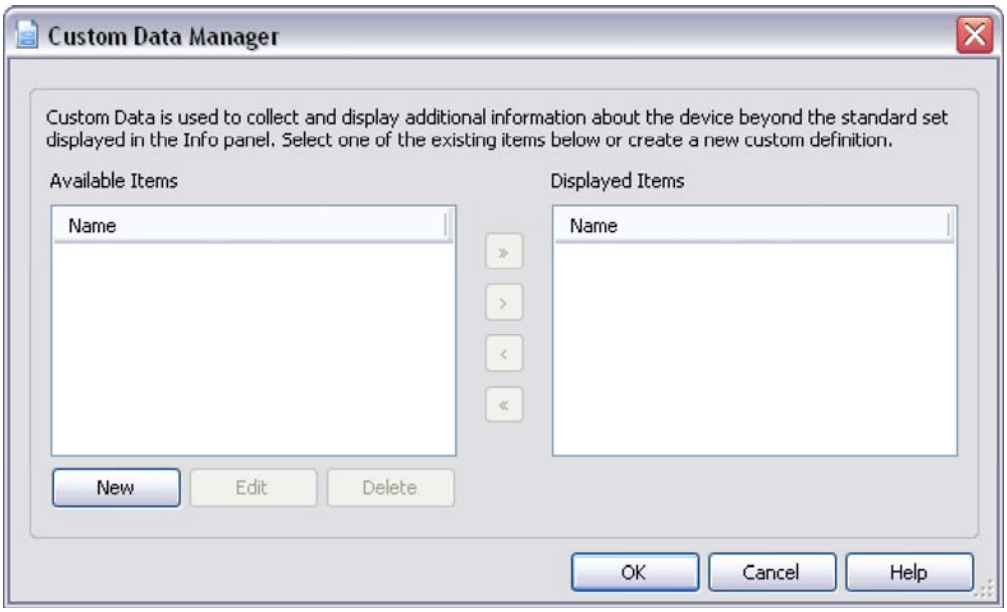
- The **Notify Server on Application Termination** option will generate a log event on the server and display it in the Event Logs for that particular device when an attempt is made to run a blocked operation. Device logs can be viewed in the MobiControl Manager by highlighting the device or the group of devices and enabling the **Logs** tab. This allows the administrators using MobiControl Manager to track any attempts by the end users to run or install unauthorized applications and ensures a higher level of monitoring.
- The **Notify User on Application Termination** option causes a message box to be displayed on the user's device when an application is blocked.

NOTES:

- When logged in as Admin on the mobile device, application control enforcement is suspended.
- Certain processes and applications are critical and necessary for stable device operation and normal execution of the MobiControlDevice Agent. These processes are automatically protected through a built-in "permanent white list" and cannot be put on a black list. Applications that are included in a lockdown program menu are automatically on a white list, and cannot be put on a black list.

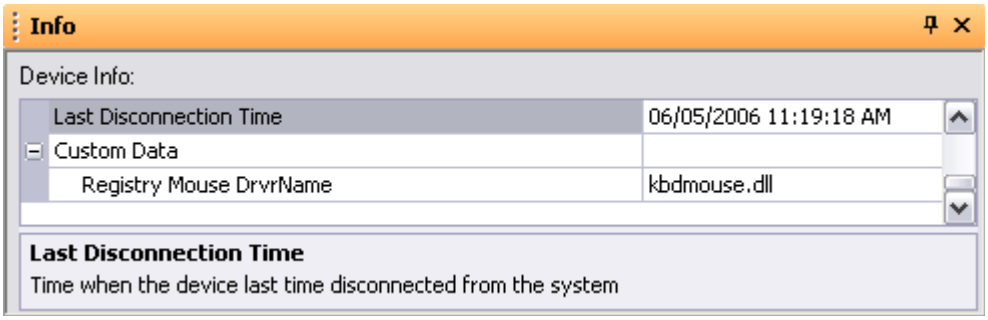
Custom Data

The custom data feature in MobiControl allows users to create their own monitoring fields to be shown in the **Device Info** window. This can be useful for monitoring various aspects of third-party applications. Custom data values are refreshed from the device when the device reconnects to the MobiControl Deployment Server and periodically, while the device status is Online, based on the device update schedule.



Custom Data Manager

The Custom Data Manager is accessible by right-clicking on a device or group, then selecting **Configure Device(s)** and clicking **Custom Data**.



The Device Info panel in MobiControl Manager

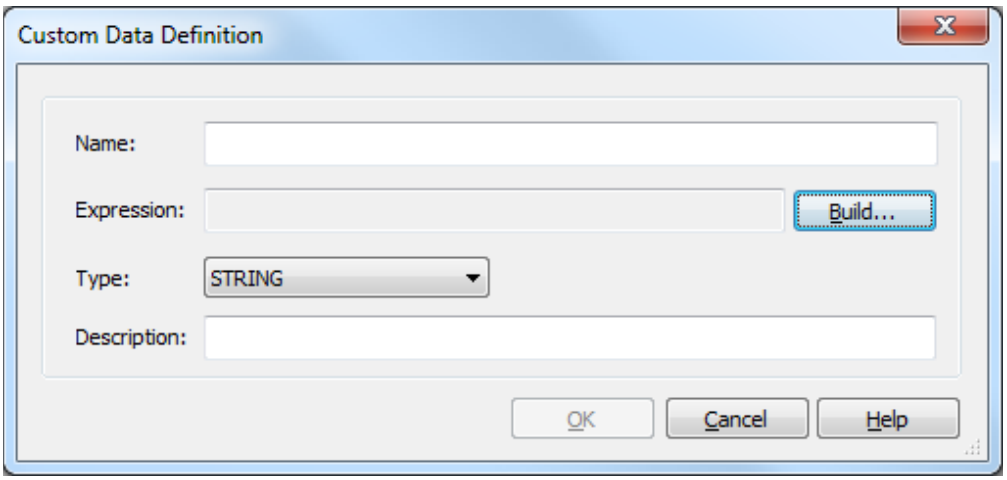
The following custom data types are available:

Type	Format and Description	Example
Text File	<Key>=TXT://\<FileName>?LN=<ValueNumber> Get the content of specified line of the text file (if LN is not specified, it assumes the first line)	TXT://\Device.log?LN=1
Registry	<Key>=REG://<GlobalKeyName>\<RegistryKey>?VN=<ValueName> Get a value from the registry. <GlobalKeyName> can be one of: • HKEY_CLASSES_ROOT • HKEY_CURRENT_USER • HKEY_LOCAL_MACHINE • HKEY_USERS	REG://HKEY_LOCAL_MACHI VN=Version
.INI File	<Key>=INI://\<FileName>?SC=<SectionName>&NM=<ValueName> Get a value from a Section in an .ini file.	INI://\SOTI\pdb.ini?SC
Exit Code	<Key>=EXE://\<Executable>[<ArgumentList>] Get the exit code of the executable	EXE://\windows\system3
STDOUT	<Key>=STDOUT://<Executable>[<ArgumentList>] Get the first line of STDOUT output of the executable.	STDOUT://cmd.exe /c di
Static	<Key>=Text Enter the static value to display in the device info pane. This information is not based on any value on the device but based on user input.	OwnerName="X & Y Corpo

Editing Custom Data

Configuration of custom data entries is performed through the Custom Data Manager which can be accessed by highlighting the device or the device group and selecting **Custom Data** from the **Configure Device(s)** option in the **Device** menu.

You can use the buttons in the **Custom Data Setting Manager** dialog box to add new entries, edit existing entries and change the order position of the custom data entries as displayed in the **Info** window.



Custom Data Definitions window

The following table describes the fields in the **Custom Data Definition** dialog box.

Field Name	Description
Name	Name of the custom data field that you want to show in the device info pane
Expression	The build button can be used to create a definition which will be used to collect the custom data values.
Type	Default is set to "String." This setting is only recommended when doing custom data collection. Other options are "Float" and "Integer."
Description	A brief note describing the nature of the custom data query and its purpose. This description is shown in the device info pane when the custom data field is selected.

Custom Data: Text Files

The following table describes the fields in the **Custom Data Type: Text File** dialog box.

Field Name	Description
Text File Name	Specify the location of the text file on the mobile device.
Line Number	Specify the line number that should be read from the text file and displayed in the device info pane.

Custom Data: Registry

The following table describes the fields in the **Custom Data Type: Registry** dialog box.

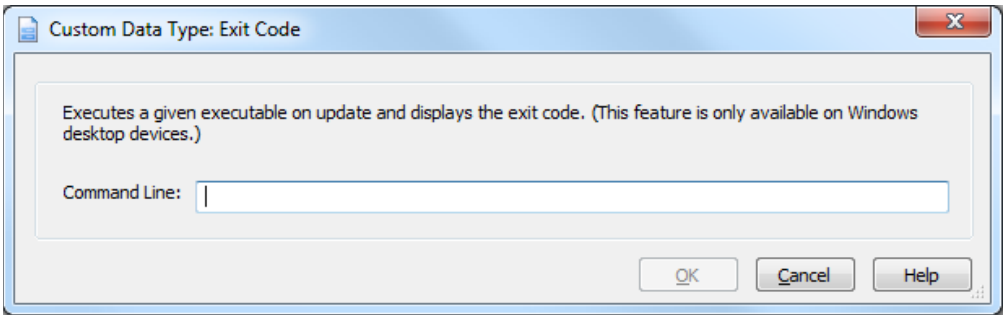
Field Name	Description
Registry Hive	Specify the registry hive where the information is located.
Key Path	Specify the exact path of the value that needs to be read.
Value Name	Specify the name of the value that should be ready and displayed in the device info pane. **NOTE:** Only REG_SZ and REG_DWORD value types are supported.

Custom Data: .Ini File

The following table describes the fields in the **Custom Data Type: INI File** dialog box.

Field Name	Description
INI File Name	Location of the `.ini` file on the mobile device
Section Name	Section from which the value should be read
Value Name	Value that should be read from the `.ini` file and displayed in the custom data field in the Device Info panel

Custom Data: Exit Code



The following table describes the field in the **Custom Data Type: Exit Code** dialog box.

Field Name	Description
Command Line	Display the exit code of the application or command line instructions once they are executed.

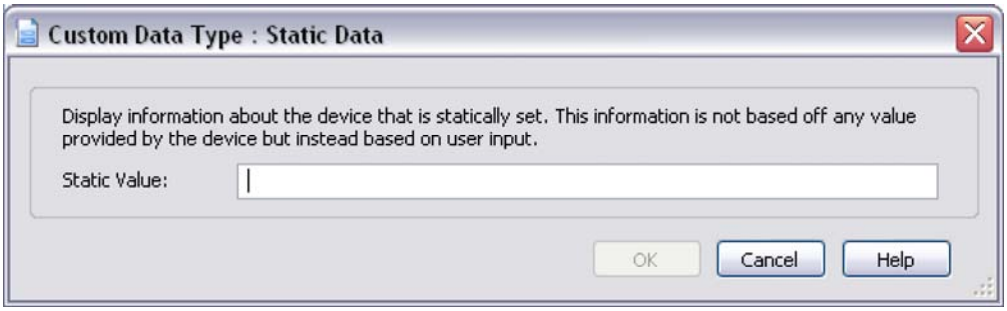
Contact us

Custom Data: STDOUT

The following table describes the field in the **Custom Data Type: STDOUT** dialog box.

Field Name	Description
Command Line	Enter the command line instructions that should be executed and the first line of the return is displayed in the device info pane.

Custom Data: Static Data



The following table describes the fields in the **Custom Data: Static Data** dialog box.

Field Name	Description
Static Value	Enter the static value here to display in the device info pane. This information is not based on any value on the device but based on user input.

Embedded Query

A query string can be in another query string by using the format %<KeyName>%. The embedded query must be defined before the query. It works only in static type query and there has to be one static custom data type for every embedded query.

EXAMPLE:

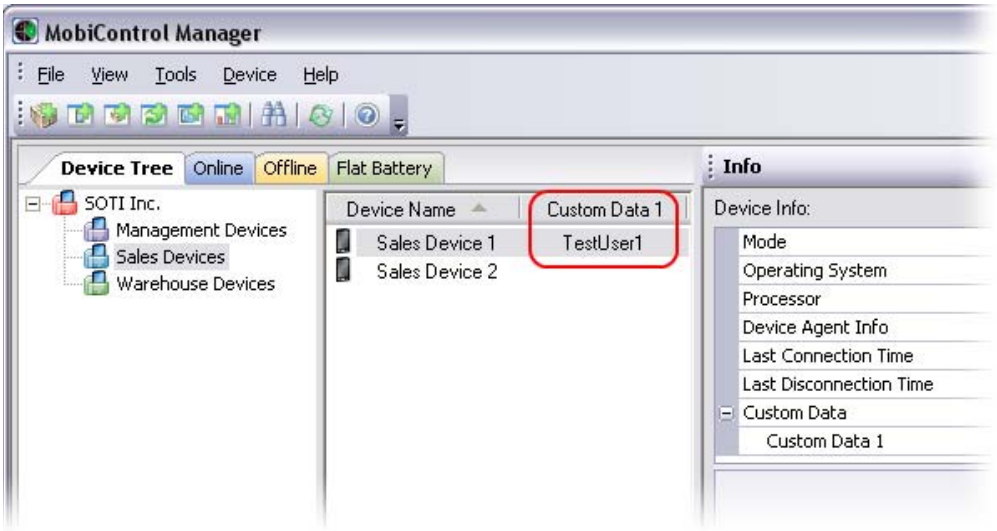
```
Key1=TXT://\RegLocationSSID.txt?LN=1
Key2=REG://%Key1%
```

Limitations

- All result values are limited to 250 characters. They will be truncated if this limit is exceeded.
- All Query Key Names are limited to 80 characters.
- All query strings (URLs) are limited to 250 characters.
- Typing "STDOUT" works on DOS and Desktop Agent. It doesn't work on CE and Pocket PC Agent.

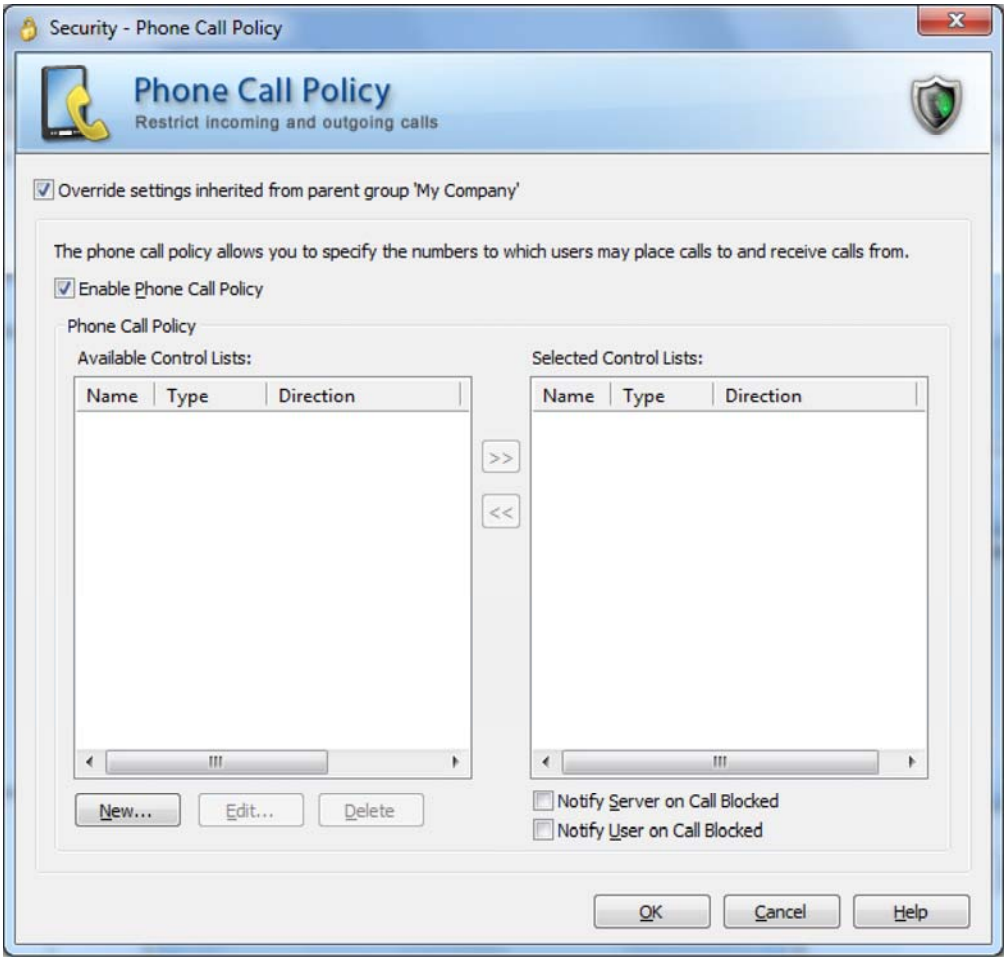
Custom Data Device Column

Once custom data has been configured, you can display or hide these custom data. Right-click on the device tree header or white space in the device tree and select **Custom Data**. You can also choose to display or hide the predefined data values displayed in the list.



Phone Call Policy

MobiControl provides various on-device feature controls including the capability to block various device communications, including what numbers a device is able to call or receive calls from.



Phone Call Policy dialog box

For assistance with Override Settings Click Here.

Contact us

Phone Call Policy Control Lists

MobiControl allows you to specify the numbers to which users may place calls to and receive calls from:

1. The **Available Control Lists** displays all control lists that have been defined, but currently are not in use. IT administrators are able to create several different phone call policies without having them be activated on the devices.

NOTE:

You can't have both deny and allow control lists activated at the same time. All control lists for a particular direction must be the same type.

2. The **Selected Control Lists** displays all currently activated control lists. Only the control lists included in the selected control lists are allowed to execute on the device. This provides an added layer of security for organizations concerned about unknown phone calls that may be placed from or received by the device. This can potentially happen without the end user being aware of it, as is frequently the case with viruses, spyware and other malicious applications.

IMPORTANT:

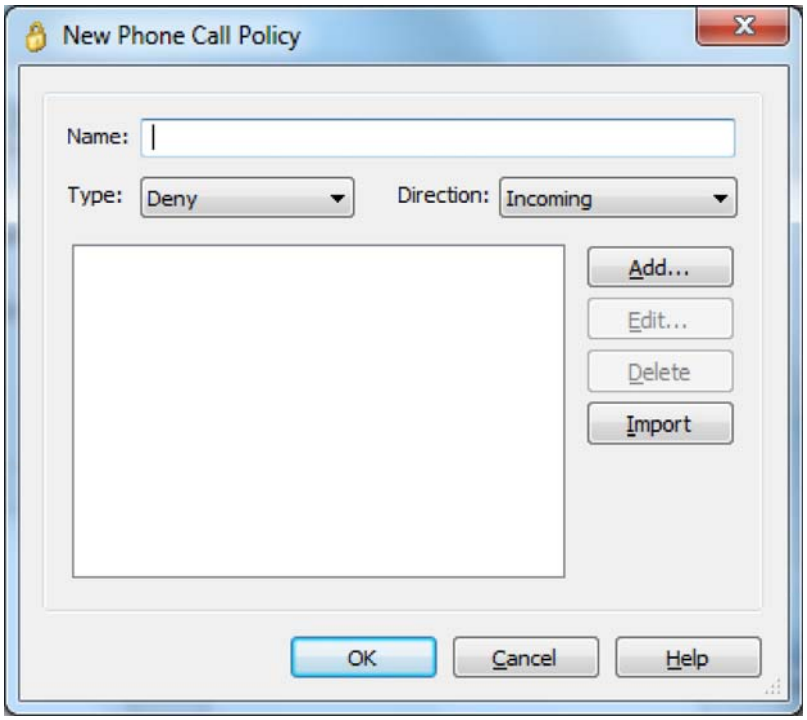
If the allowed list is not set up correctly, you may end up blocking or not allowing a potential system critical phone call.

3. When the **Notify Server on Call Blocked** check box is checked, the server's log file will output all calls that were blocked, along with the phone number that was trying to call in or out for the particular device.

4. When the **Notify User on Call Blocked** check box is checked, and the user receives an incoming call from a phone number that was blocked, a message box will be displayed

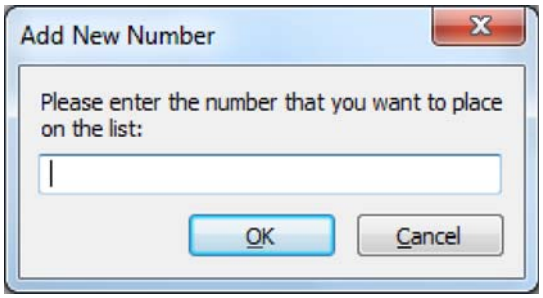
To enable phone call policy control for a device or group of devices, select **Phone Call Policy** from the MobiControl Security Center. (Please see the Device Security and Control page.)

Contact us



New Phone Call Policy entry dialog box

Field Name	Description
New	Clicking on this button allows you to create a new phone call policy with the dialog box as shown above. Assign a meaningful name to help distinguish between the various phone call policies you may setup.
Type	The available options allowed are either Allow or Deny. The type Allow indicates the phone calls that can either be placed from the phone or received by the phone or both based on Direction set for this policy. The type Deny indicates the phone calls that can not either be placed from the phone or received by the phone or both based on Direction set for this policy. If attempting to block restricted or unknown callers simply add **<Unknown>** and/or **<Restricted>** to the deny list.
Direction	The available options are Incoming, Outgoing, or Both. Incoming indicates that this policy is for calls received by the device. Outgoing indicates that this policy is for calls placed by the device. Both indicates that the policy is for both incoming and outgoing calls. For example, you may want to allow all communication to and from your device to your IT Support team and hence you would select both in this case with the appropriate phone numbers that can be dialled to work with your support team.



Add Phone Call Policy entry dialog box

Once you have configured the Name, Type and Direction, click on **Add...** in order to enter in the phone number(s) that the policy applies to and the dialog box is displayed above.

MobiControl will compare the number either received or placed with the list of numbers mentioned in the policy and compare the exact phone number displayed with the list of numbers you provide. If you have a series of numbers that you would like to enter in, there are a few options available, which can be used in combination with each other:

1. Leverage the wild card character, which is the asterisk, or '*'. The asterisk indicates any number of digits. For example, you may want to only allow calls coming from a particular area code. In this case, you can enter in '<area code>*' as the number.

   EXAMPLE:

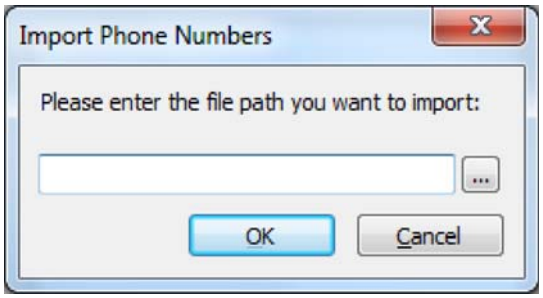
   416* would match all calls that start with 416.

2. Leverage the single wild card character, which is the question mark, or '?'. The question mark indicates any single digit.

   EXAMPLE:

   You may want to allow communication to a list of phone numbers that only vary by a single digit. In this case, you can enter in as an example, 444-555-123?. This indicates the policy applies to the following list of numbers:
   444-555-1230
   444-555-1231
   444-555-1232
   444-555-1233
   444-555-1234
   444-555-1235
   444-555-1236
   444-555-1237
   444-555-1238
   444-555-1239
   Combinations of the two wild card characters can also be used if required. For example, 4??-555-12* would succeed if the phone number is 432-555-1234, but not if the phone number is 432-432-1234

 Contact us



Import Phone Call Policy entry dialog box

When the **Import** button is selected, the dialog box above is displayed. From here you can select any file type. MobiControl assumes that the input file format is **one phone number per line**.

EXAMPLE:

905-888-8888
519-222*
416*
Upon reading in the file, the individual numbers will be added to the list control, just as though they were individually typed in using the Add button.

IMPORTANT:

The file being imported must not contain more than 2000 lines.

Contact us

Creating Device Relocation Rules

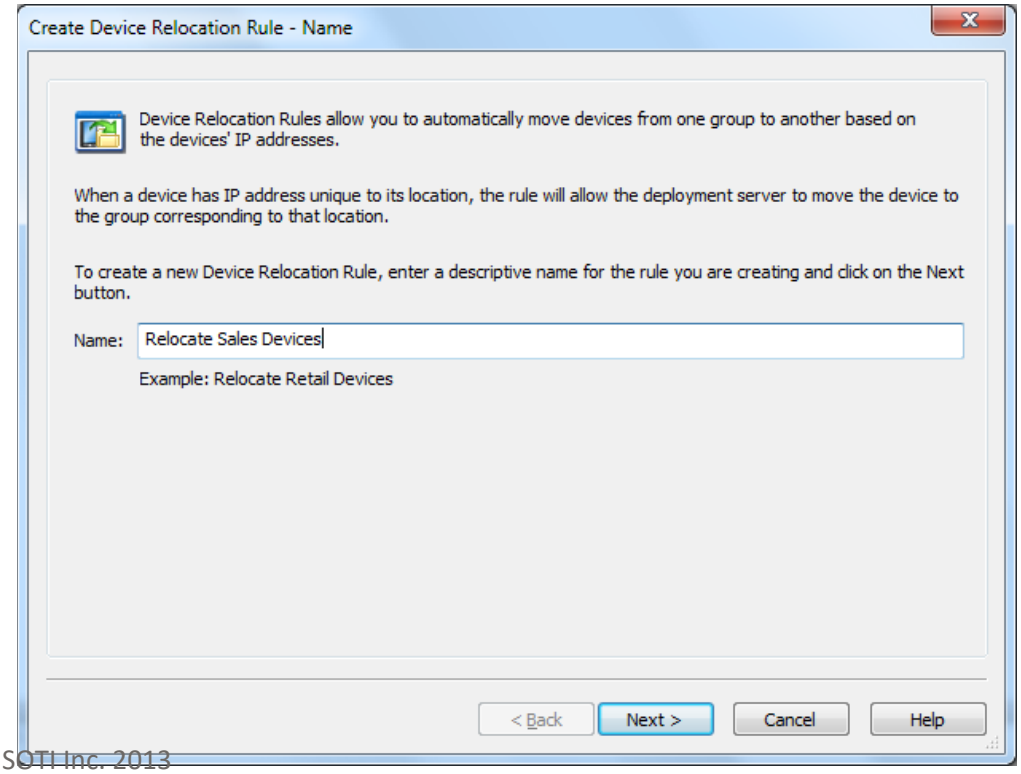
Dynamic device relocation allows you to set up rules to move your mobile devices automatically between different virtual groups or device groups in the MobiControl device tree based on the IP address or other custom criteria. This is useful when managing mobile devices in a deployment where the device tree is set up to represent different physical locations (e.g. retail stores, warehouses, regional offices, etc.).

In a deployment that has mobile devices connecting from and moving frequently between several different sites, properties or regions, the administrator needs visibility over the movement of mobile devices across different locations. Dynamic device relocation allows the MobiControl device tree to be updated automatically when a device moves to a different location (e.g. a mobile device that has moved from a warehouse or site in Chicago to a site in New York will automatically be relocated in the device tree on reconnection and will appear in the device group for devices in New York based on the new IP address information). Additionally, the devices can also be automatically reconfigured and any modifications to the mobile device settings, specific to the new location, will be sent to the device automatically.

The devices are relocated based on the IP address ranges specified for each location. You can also create a custom data identifier which can be the criterion that will be utilized to relocate the devices to the appropriate device group. (Please see the Custom Data page for detailed information on custom data identifiers.)

1. Start the wizard.

   From MobiControl Manager, select the Rules view (tab), then click **Rule,** select **Create Rule,** and click **Create Device Relocation Rule.** The first page of the Create Device Relocation Rule Wizard will be displayed. Enter a meaningful name for the rule and click **Next** to continue.



 Contact us

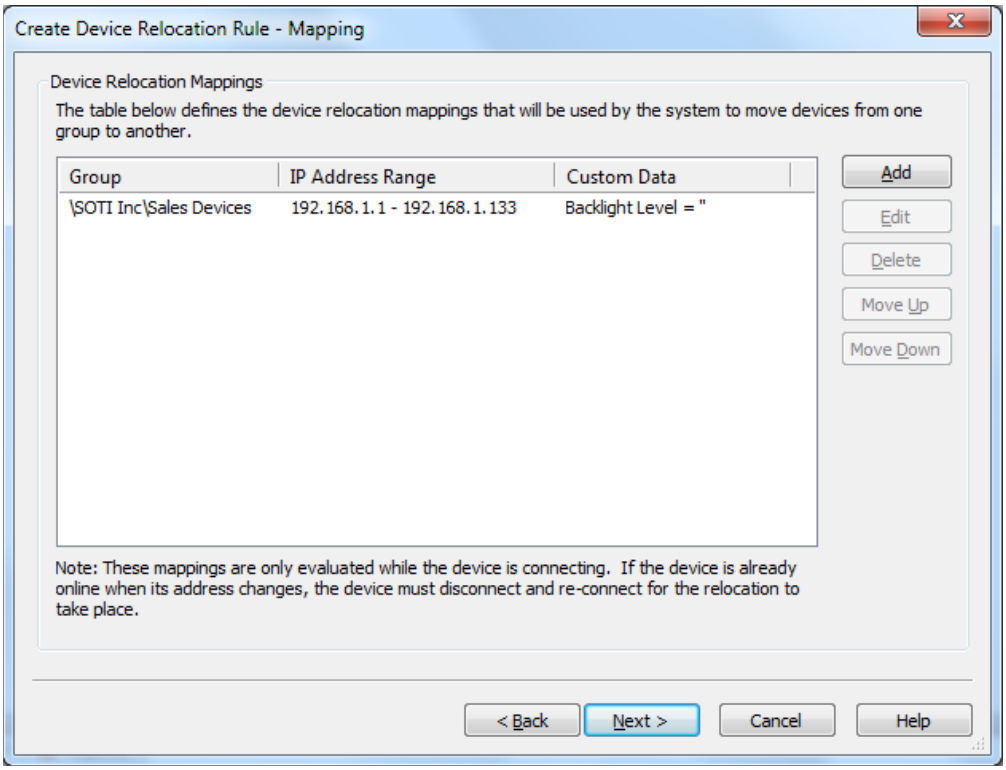
*Create Device **Relocation** Rule Wizard startup dialog box*

2. Review the device relocation mappings.

This page lists **device relocation mappings** that determine how the devices would be relocated and in which groups they would appear if the specified criteria is met. When a device connects to the MobiControl Deployment Server, its IP address and custom data information will be checked against all device relocation rules configured, and it will be moved to the appropriate device group based on the information in the relocation mappings.

NOTE:

Devices that are already connected and online in MobiControl will be relocated when they disconnect and re-connect to the MobiControl Deployment Server.



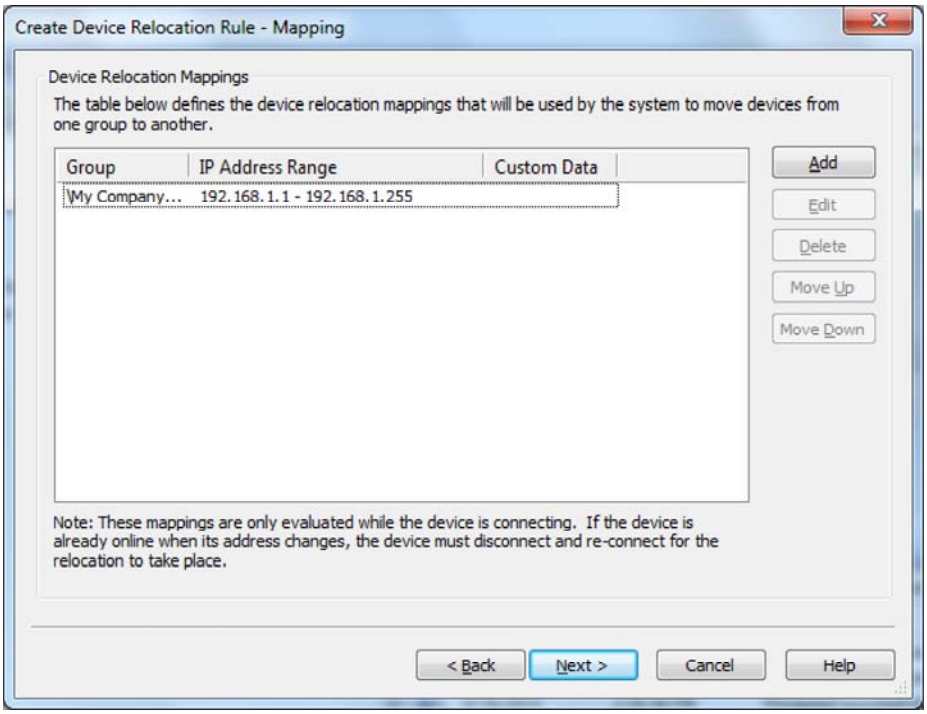
*Edit Device **Relocation** Rule dialog box*

The buttons on the **Edit Device Relocation Rule** dialog box are explained below:

Button Name	Description
Add	Click the **Add** button to add an entry for the relocation mapping.
Edit	Click the **Edit** button to change the settings for an existing relocation mapping entry.
Delete	Click the **Delete** button to delete a relocation mapping entry.
Move Up / Move Down	

Button Name	Description
	Click these buttons to change the order of the relocation mappings. The entry listed higher in the list have a higher priority and take precedence over entries listed lower in the list. For more details, read about relocation mappings priority below.

A relocation mapping can use just the IP address or the custom data entry to specify the relocation rule for mobile devices. If a relocation mapping has both the IP address and custom data entry specified as the criteria, the mobile devices would be relocated only if both these conditions are satisfied. If a device is affected by more than one relocation mapping, the one higher in the list of mappings will have a higher priority and will be effective. You can use the **Move Up** and **Move Down** buttons to change the precedence of the relocation mappings if multiple mappings apply to a device.



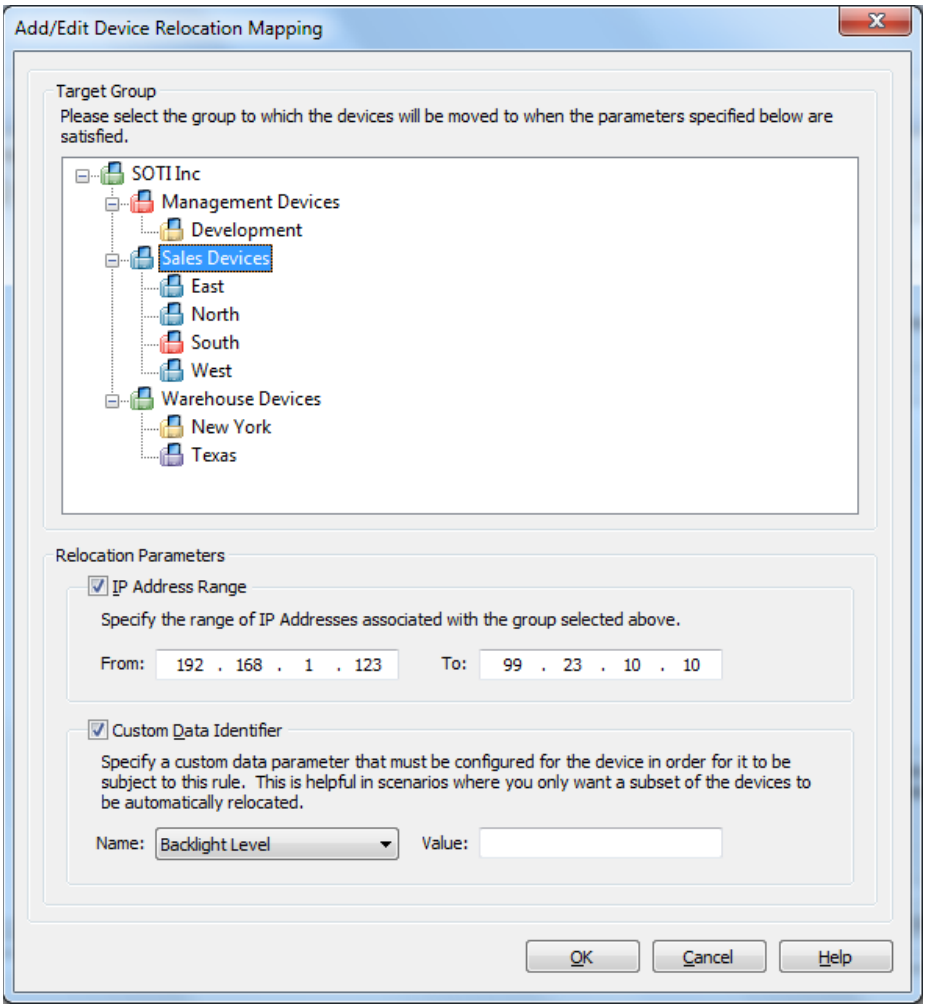
*Device **Relocation** Mappings dialog box*

The first two relocation mappings in the previous screenshot have been defined: one is for relocating all devices with IP addresses between 192.168.1.1 and 192.168.1.255 to the Management Devices group and another mapping for relocating all the devices for which the custom data item "Location" has a value of "Region A" to the Warehouses group. Since the relocation mapping with the IP address filter is listed above the mapping with the custom data filter, the IP address mapping will take precedence. If a device satisfies both conditions (e.g. has an IP address 192.168.1.10 and a value "Region A" for "Location"), it will be relocated to the Management Devices group.

 Contact us

3. Add or edit device relocation mappings.

A relocation mapping includes the target or destination group (which can be a virtual group) to which the devices would be relocated. It also includes the conditions or the relocation parameters that must be satisfied for a device to be relocated.



*Add/Edit Device **Relocation** Mapping dialog box*

The **target group** is the group, sub-group, or virtual group to which devices will automatically be relocated when connecting to the Deployment Server if the conditions specified in the relocation parameters are met.

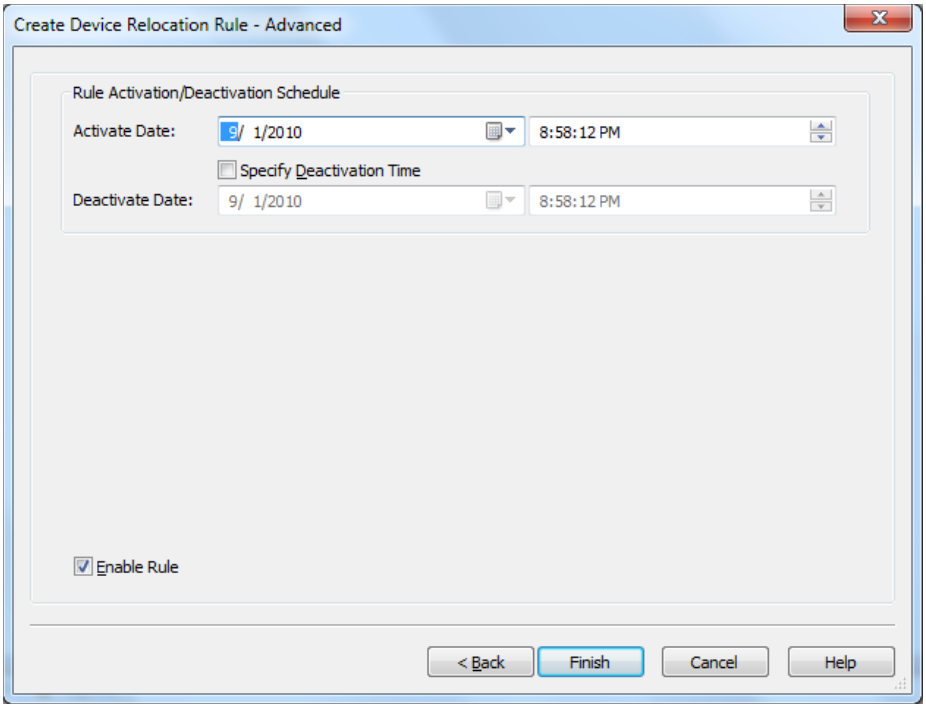
Multiple **relocation parameters** can be specified to manage the dynamic relocation of devices. A single parameter can be specified or both parameters can be used for a relocation mapping, in which case the device will be relocated if it satisfies both parameters.

The following table describes the fields of the **Add/Edit Device Relocation Mapping** dialog box:

Field Name	Description
IP Address Range	

Field Name	Description
	Devices can be automatically relocated based on the IP address information of the device at the time it connects to a Deployment Server. A range of IP addresses can be specified and if the device's IP is within that range, the device will be relocated to the target group.
Custom Data Identifier	You can use a custom data value as one of the criteria for relocating devices from one device group to another. MobiControl allows you to retrieve arbitrary data from the device's registry, files on the device and other sources using custom data. Please see the Custom Data page for more information.

4. Specify the rule activation or deactivation schedule.



*Edit Device **Relocation** Rule Activation/Deactivation Schedule dialog box*

By default, the device relocation rule will be activated immediately upon completion of the wizard. If you wish to delay the activation, you can modify the activate date. A deactivate date can optionally be entered to specify a date from which the rule will be disabled.

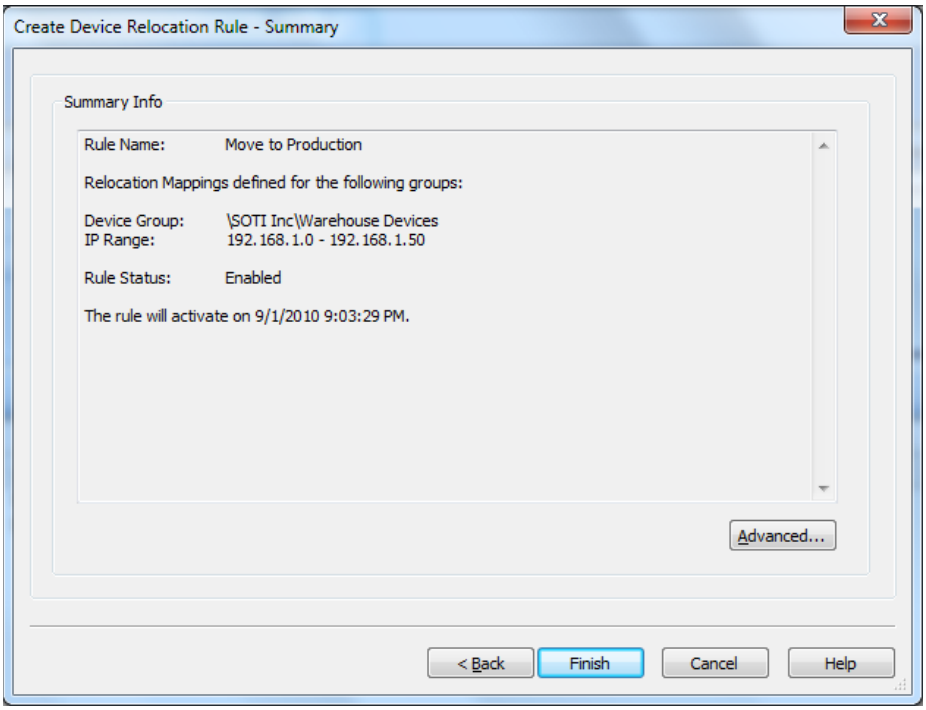
A device relocation rule can also be explicitly disabled by clearing the checkbox next to **Enable Rule.**

After entering the fields in the above dialog box, click the **Next** button to continue.

 Contact us

5. Review the summarized settings.

This page gives you an opportunity to review the settings of the device relocation rule before committing them to the database. If you wish to make any corrections, click the **Back** button, otherwise click **Finish** to complete the wizard.

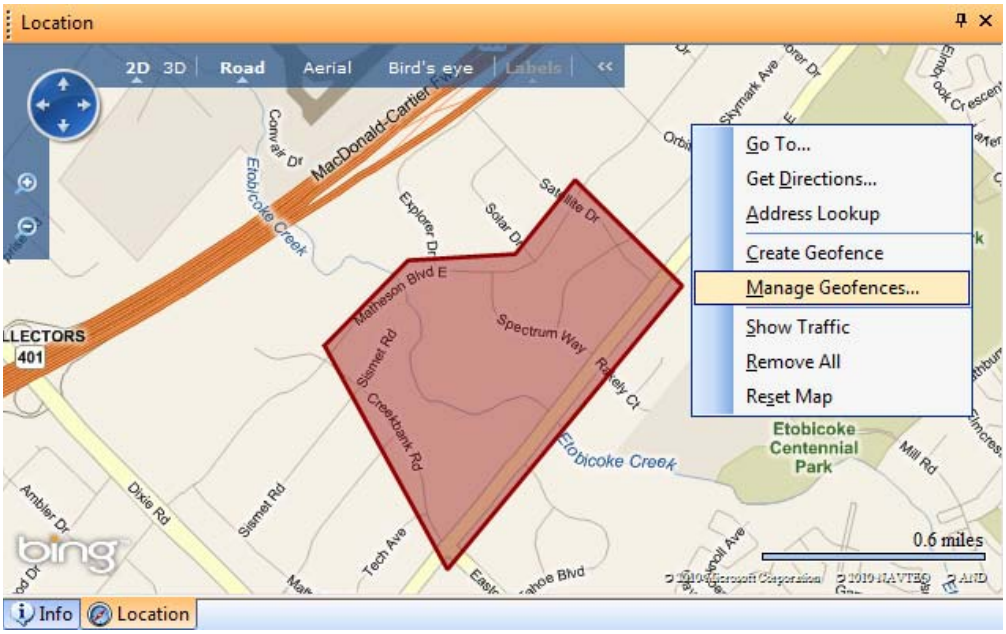


*Edit Device **Relocation** Rule Summary dialog box*

Contact us

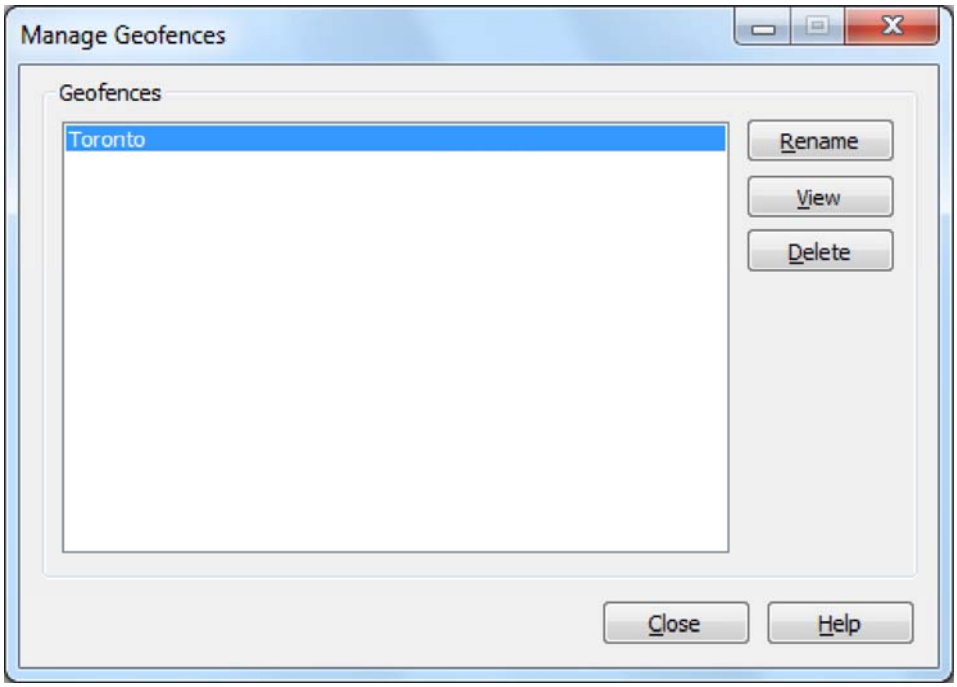
Using Manage Geofences

The Manage Geofences feature provides an area in which to rename, delete or view current created Geofences. You also have the option to create a new geofence from the drop down menu.



*Location panel right click map and select **Manage Geofence** option*

Selecting Manage Geofence brings up the following window.



 Contact us

Field Name	Description
Rename	Allows you to rename a Geofence
View	Allows you to view an already created Geofence on the map
Delete	Allows you to delete a Geofence **NOTE:** In order to Delete the Geofence, no Geofence Event can be associated with it

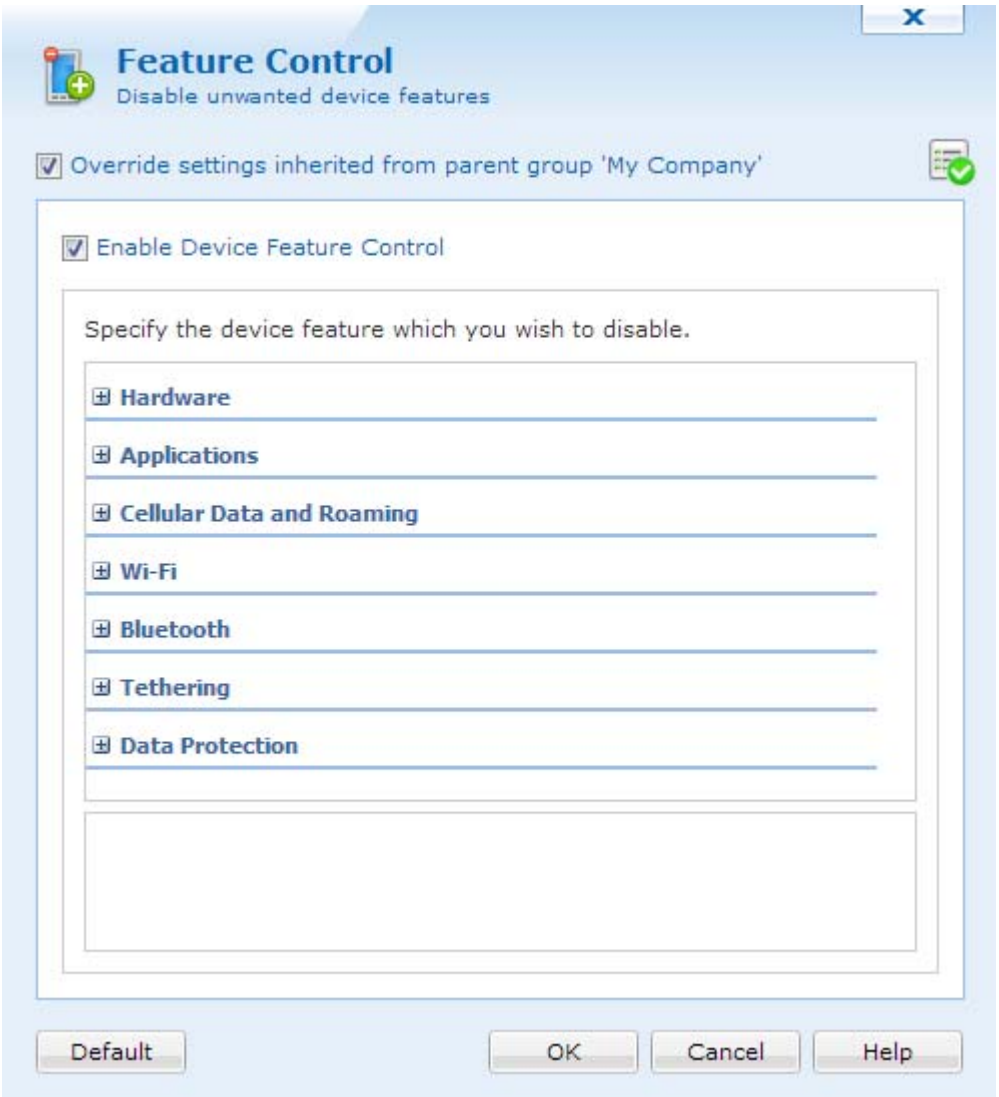
The **Create Geofence** option allows you to begin drawing on the map. The area drawn on the map will be defined as the Geofence. The defined area must be a complete geometric shape, which means the Start Drawing point will be the same as the End Drawing point. When you have completed a proper geometric shape you be asked to name your geofenced area.

Contact us

Android+ Device Feature Control

For security-conscious organizations and environments where privacy and information security concerns require controlling the unauthorized transfer of mobile data out of the mobile devices, MobiControl provides various on-device feature controls including the capability to block various device communications, similar to firewall functionality. MobiControl's device features control policy allows IT administrators to selectively disable device features. Applying the policy at the individual or group level allows custom profiles for different users and locations in an organization. The ability to disable or enable Bluetooth and infrared ports allows controlling whether end users can beam business cards, applications or documents to one another.

To enable the device feature control, right click a device or group of devices, and select **Device Configuration**. Once the Device Configuration dialog appears, click **Feature Control**.



*Device **Feature** Control Policy dialog box*

Contact us

NOTE:

Some device feature controls may not work with all MDM versions. To see what MDM version is on your device, select the device in the web console and expand the info panel. Scroll down until you see Supported APIs.
To see which features are supported by your MDM version, click 

The following features can be enabled or disabled using the device feature control policy. The list is organized by OEM's certified for MobiControl:

- **LG**
- **Lenovo**
- **Pidion**
- **Huawei**
- **Honeywell**
- **Motorola**
- **Panasonic**
- **Samsung**

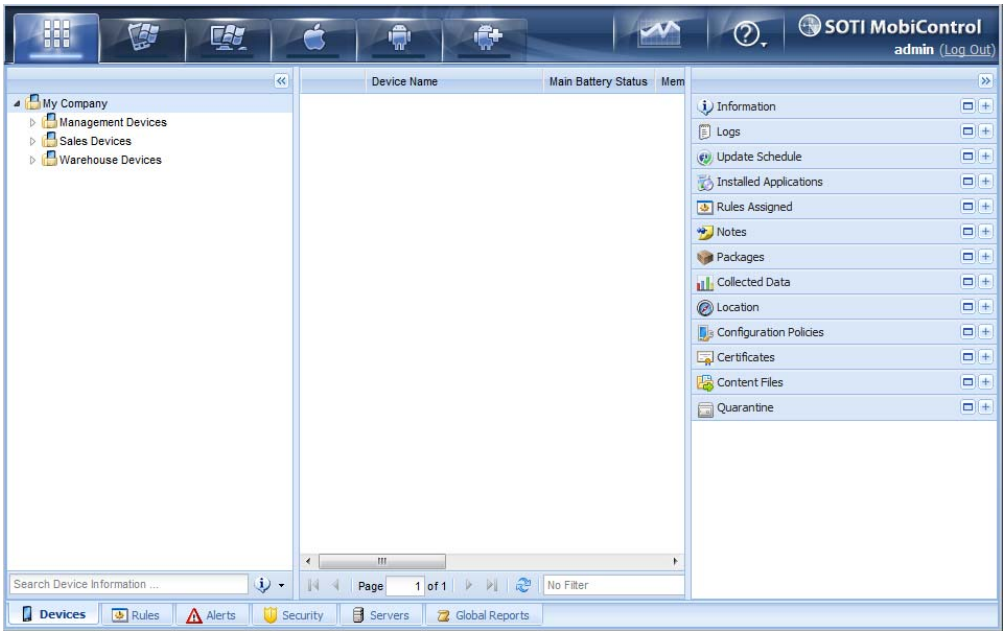
Contact us

MobiControl Web Console

The MobiControl Web Console allows you to provide Management Console access to your mobile support team using a thin management console available anywhere where Internet Explorer is installed.

The Web Console is an online Management Console providing you with the ability to support your mobile devices from anywhere in the world. You can do everything from locate your devices to remote control, and even send scripts.

The MobiControl Web Console is installed to https://localhost/MobiControl



From the MobiControl Web Console you can:

- Remote Control/View
- Send Scripts and Messages
- Locate and Track Devices
- View Logs, Device Info, Packages, Assigned Rules and Installed Programs
- Make Notes
- View Deployment Server Information
- Generate Reports

NOTE:

When using remote control on the Web Console, MobiControl will ask you to download a special .MSI file that contains the remote control package. After installing the .MSI, you will need to restart your browser. This allows you to remote control devices in Chrome, Firefox, Safari (Windows only) and Internet Explorer.

 Contact us

Device Status Icon

The MobiControl Web Console allows you to identify the different devices and their states via the device icon. The table below references the different icons and their states

Device	Description	Icon
Windows CE / Windows Mobile device	Online	
	Offline	
	Learning	
Windows Desktop device	Online	
	Offline	
Apple iOS	Online	
	Offline	
	No Device Agent	
	Error - Profiles not installed	
Google Android	Online	
	Offline	
	Error - No Administrator rights	

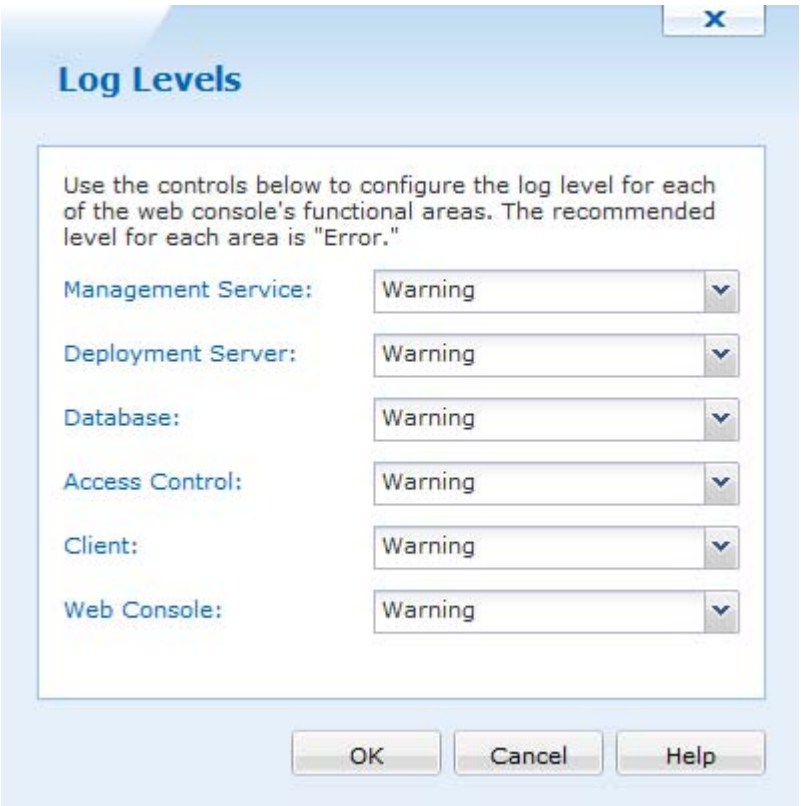
Logging

The web console has the ability to set logging levels and to view the log file generated.

Log Levels

To set the log levels, click the question mark on the top right hand corner, and select **Log Levels**. The logging levels can be set for the Management Service, Deployment Server, Database, access control, client or Web Console. These files are stored on the computer where these services are installed on.

Contact us



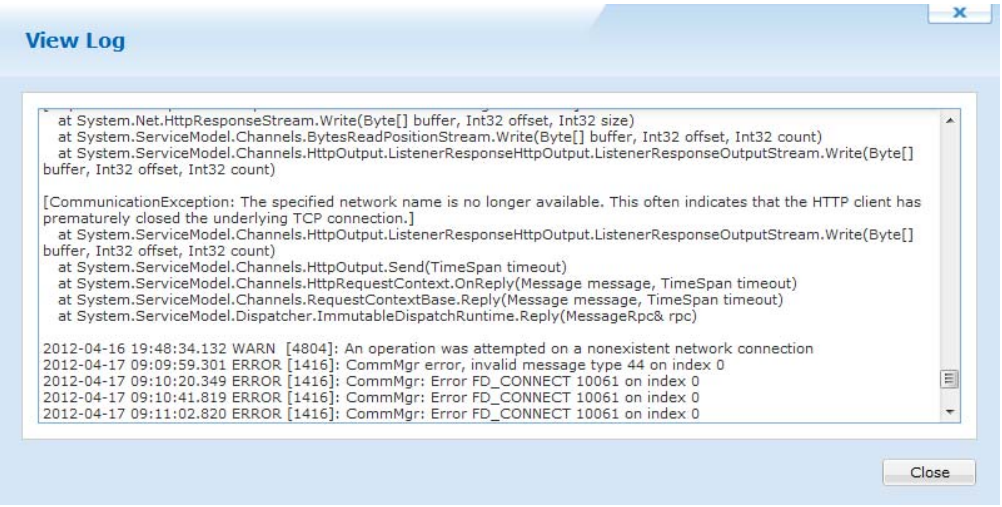
MobiControl Log Levels

Log Level	Description
Off	Setting the log level to Off turns off any logging for the associated section.
Error	Setting the log level to Error allows only error messages to be written to the log file
Warning	Setting the log level to Warning allows only warning messages to be written to the log file
Information	Setting the log level to Information allows only information messages to be written to the log file
Verbose	The Verbose setting enables Error, Warning and Information to be written to the log file at the same time.

View Log File

To view the log file in the Web Console, click the question mark on the top right

hand corner, and select **View Log Levels.**



MobiControl log file

 Contact us

MobiControl Release Notes

v14.1 — Build 1157 — April 2, 2018

v14.0 — Build 4905 — October 31, 2017

v13.4 — Build 3193 — November 2, 2017

v13.3 — Build 2906 — December 30, 2016

v13.2 — Build 3081 — August 31, 2016

v13.1 — Build 5200 — May 16, 2016

v13 — Build 33604 — December 31, 2015

v12.4 — Build 30627 — September 25, 2015

v12.3 — Build 28275 — July 28th, 2015

v12.2 — Build 21409 — May 27th, 2015

v12.1 — Build 22592 — February 27th, 2015

v12 — Build 185 41 — December 19th, 2014

v11 — Build 14250 — May 7th, 2014

v10.0 — Service Pack 1 — August 27th, 2013

v10.00 — Build 9529 — January 7th, 2013

Upgrade Observations

- After upgrade all LDAP connections will require re-configuration of Base DN and Authentication Type
  - If using LDAP Authentication for Console Security, ensure that the local administrator account is known prior to upgrading
- After upgrade Console Security must be managed through Web Console (option has been removed from MobiControl Manager)

Release Highlights

- Introduces completely redesigned Apple® iOS and Google Android™ device agents featuring:
  - Content Library
  - Application Catalog
  - Support Contact Details
  - Terms & Conditions
  - Message Center
  - Location Discovery (iOS)
  - Device Configuration Summary
- Introduces Secure Content Library with support for:
  - Pushed or On Demand distribution of content to device agents
  - Effective and Expiration dates for distributed content
  - File Sharing Restrictions (iOS)
  - Content Categorization
  - Versioning
- Introduces Telephone Expense Management with support for:
  - Monitoring, reporting, and alerting on Data usage (All Mobile Platforms) and Voice usage (Windows Mobile, Android)
  - Adds support for Phone Call Policy and Call Logs (Android)
- Introduces Certificate Management with support for:
  - Device certificate inventory
  - Integration with Microsoft PKI (ADCS), and Entrust Certificate Authorities for the request and subsequent distribution of certificates (All Mobile Platforms)
  - Support for dynamic and static challenge SCEP payloads (iOS)
  - Automatic certificate renewal
  - Certificate revocation (when using ADCS via DCOM)
  - Association of Certificate to WiFi, VPN, Email Device Configurations for Authentication or Encryption
- Introduces customizable and versioned Terms & Conditions for end user acceptance during enrollment
- Introduces Speed-sensitive Lockdown to customize Lockdown screen when device is travelling faster than defined speed (Android, Windows Mobile)
- Enhanced Remote Control featuring Bit4ne tile for up to 10x faster Remote Control
  - Remote Control Console now opens as an applet, and is no longer IE dependent
  - Remote Control Console will attempt to detect the device model and choose the appropriate device Skin (available in most cases)
- Introduces Anti-Virus/Malware protection via WebRoot (Android)
- Introduces Categorized Web Filtering via WebRoot (Android)
- Adds support for Microsoft®Windows 8 Desktop

General Features

- Enhancements to LDAP integration to support manual specification of Search Patterns and LDAP attributes. Includes support for Open Directory, Domino and other LDAP servers.
- Optimized performance of File Transfer protocol
- Adds support for sending a message to the Device Ico on Alert Rule action
- Adds support for Management Server to communicate outbound through a proxy via configuration file entry
- Adds support for Geofence under Alert Rules (Android, iOS)
- Enrollment can now be achieved without Enrollment service by entering Server Address, Rule Tag and Site Name (Android, iOS)
- Redesigned Installer featuring detection of current installed state to streamline installation / upgrade process

Web Console Features

- Introduces Custom Attributes to support adding additional fields to Web Console
- Redesigned Device Configuration panel (formerly Security Center)
- Adds support for applying Notes to Device Groups and Virtual Groups
- Introduces support for using Macros in Device Configuration dialogs that require values for Username and Email
- Minor changes to Rule cards to streamline configurations
- Web Console will now display a device's associated user in the Info Panel
- Introduces dialog for manually changing a device's user association
- Added support for creating and editing "Filter" views
- App Catalog configuration now supports discovery of Apps through Google Play (Android)
- Introduced "Configuration Policies" info panel to indicate the Device Configurations assigned to device.
- Agent Connected/Disconnected state is now shown indicating how long the Agent has been in this status
- Global Settings now displays the Database Connection String
- Adds support for opening all Info Panels in Maximize View
- Introduces method to dismiss yellow console alerts
- Web Console URL address can now be customized during installation
- Added additional Console Security permissions related to new features
- Introduces progress bar during Agent Creation when using Agent Builder Service
- Device Info Panel now indicates the active connection type (WiFi/3G etc.)
- Passcode status is now displayed in the Info Panel (Android)
- Internal/External Encryption status is now displayed in the Info Panel (Android)
- WiFi signal is now displayed in percentage (%) as well as dB. (Windows Mobile, Android)
- Hardware Serial Number and OEM Version are now displayed in the Device Info Panel for Android+ devices
- Add Device Rule filters now support filter by IP Address (iOS, Android), removes filter option for "Agent Name" (Windows Mobile)
- Renamed Right-Click option "Refresh Device Status" to "Request Device Check-In" to adequately represent the action's behavior
- Reorganized Right-Click menu options on Device Group level
- Adds additional Device Statuses to Alert Rule triggers such as IP Address, Cellular Carrier, OS etc. (Android, iOS)
- Introduces a Device Tree legend to describe selection colors
- Introduces support for searching for Device Groups

Apple® iOS Features

- Added the following iOS Device Configurations:
  - LDAP
  - CalDAV
  - Subscribed Calendars
  - Additional VPN configurations (F5, SonicWall, Aruba VIA, Custom SSL)
- Introduces support for installing manually-crafted "Custom Profiles"
- Introduces support for automated enrollment via Apple Configurator via .mobileconfig files
- Location Services now includes an option to configure GPS Accuracy vs Battery Performance (GPS Mode vs Significant Change)
- Introduces new APNs Certificate Signing utility for issuing and renewing APNs Certificates
- iOS Agent will now re-launch after enrollment process is complete when enrollment is initiated through Agent

Google Android™ Features

- Adds support for Time Sync policy
- Adds support for Custom Data
- Adds support for Out of Contact Policy
- Adds support for Device Relocation rule
- Introduced the following functionality via script commands
  - Restart device agent (restartagent)
  - Switch agent between foreground/background mode (foregroundmode enable|disable)
  - Create directory (mkdir, md)
  - Launch an application (start)
  - App Whitelisting (see online help)
- Introduces support for executing an intent from a Lockdown screen
- Adds support for manual distribution of certificates (Samsung, LG, and Motorola for certificates containing only a public key)
- Introduces persistent storage support for Motorola Android-based devices
- Introduces Pending Actions panel for awaiting user actions such as starting Encryption Process or Passcode Policy. Pending Actions panel will "nag" user to perform these functions.
- Adds support for GCM to C2DM has been deprecated by Google
- Introduces utility to configure WiFi while in Lockdown
- Introduces utility to configure Passcode while in Lockdown
- During Enrollment Device Administrator is now silently "Activated" when device agent is obtained from Deployment Server. Adds flag in mcsetup.ini file to alter this behavior.
- Android+
  - Added support for the following Feature Restrictions for devices supported under Android+ other than LG and Samsung:
  - Bluetooth
    - Disable outgoing calls via Bluetooth (ICS+)
    - Disable Bluetooth Discoverable mode (GB+)
    - Disable Bluetooth Tethering (ICS+)
    - Disable Bluetooth Desktop Pairing (GB+)
    - Disable Bluetooth Tethering (ICS+)
    - Disable Bluetooth Pairing (GB+)
    - Allow Limited Bluetooth Discoverable mode (ICS+)
  - WiFi
    - Disable WiFi Profiles (GB+)
    - Disable WiFi Profiles Changes (GB+)
    - Enforce Minimum WiFi Security Level (GB+)
    - Disable WiFi tethering (GB+)
  - Disable Cellular Data (GB+)
  - Disable Clipboard (HC+)
  - Disable USB tethering (ICS+)
  - Disable Google Sync/Backup (GB+)
  - Disable Access to Device Settings (GB+)
  - Enforce GPS Availability (GB+)
  - Disable GPS Mock Locations (GB+)
  - Disable YouTube (GB+)
  - Disable Browser (GB+)
  - Disable installation from Unknown Sources (GB+)
  - Disable Background Data (GB+)
  - Disable NFC (ICS+)
  - Disable USB Debugging (GB+)
  - Disable USB Mass Storage (GB+)
  - Disable SD Card Access (GB+)
  - Disable All Tethering (ICS+)
- LG
  - Added support for the following Feature Restrictions for LG devices:
  - Bluetooth
    - Disable outgoing calls via Bluetooth
    - Disable Bluetooth Discoverable mode
    - Allow Limited Bluetooth Discoverable mode
    - Disable Bluetooth Pairing
    - Disable Bluetooth Tethering
    - WiFi
      - Disable WiFi Profiles
      - Disable WiFi Profiles Changes
      - Enforce Minimum WiFi Security Level
      - Disable WiFi tethering
    - Disable USB tethering
    - Disable Google Backup
    - Disable SD Card Access
    - Disable USB Mass Storage
    - Disable Clipboard
    - Disable USB Media Player
    - Disable NFC
    - Disable USB Debugging
    - Enforce GPS Availability
    - Disable GPS Mock Locations
    - Disable Background Data

Microsoft® Windows Mobile/CE Features

- Adds support for manual distribution of a known certificate
- Adds support for configuring Fusion-based WiFi configurations from Web Console
- Introduces Support Contact Info inside device agent
- Introduces a utility that allows a device to fetch a package from an FTP server rather than the Deployment Service
- Adds support for showing Bluetooth in a Custom Navigation Bar while in Lockdown
- Electronic Serial Number (ESN) of Motorola Windows-based devices is now collected and displayed in the Info Panel of the Web Console

iOS7 Compatibility (Implemented in v10.00.9619 released on August 27th, 2013)

In line with Apple's iOS 7 update, MobiControl v10 has been updated to streamline the enrollment process while implementing new app configuration methods. This new enrollment process requires that both components: MobiControl Server, and the MobiControl App be updated to the latest versions.
The new iOS enrollment process places more emphasis on using the enrollment URL rather than an enrollment ID. By using an enrollment URL, users can take advantage of automatic App configuration, rather than typing an enrollment ID.

Old Process (Agent)	New Process
• Open App Store • Install MobiControl App • Enter Enrollment ID from Add Rule • Management Profiles Installed • Device Successfully enrolled	• Go to Enrollment URL (Add Device Rule) • Install Management Profiles • User is Prompted, Installs MobiControl App • Device Successfully Enrolled • MobiControl App is automatically configured after install

Revisions:

- Release 10 build 9912 on March 6th, 2014
- Release 10 build 9619 on August 27th, 2013
- Release 10 build 9484 on April 15th, 2013
- Release 10 build 9354 on March 20th, 2013
- Release 10 build 9329 on January 7th, 2013

v9.03 — Build 7890 — May 1st, 2012

v9.02 — Build 6270 — January 27, 2012

v9.00 — Build 5679 — September 30, 2011

v8.51 — Build 5251 — April 18, 2011

v8.50 — Build 5240 — March 22, 2011

MobiControl Home
Key Features
› Apple iOS
› SDK for iOS
› Android+
› Google Android
› Microsoft Windows
Revision History
Product Literature
Support
Videos

Android+ Technology

Advanced, consistent management and security across all Android devices.

Learn More...

Web Filtering Policy

Enforce and control web access policies to ensure secure, safe and authorized access to web content.

Learn More...

Malware Protection

Protect against malware and viruses on devices in real-time.

Learn More...

EMPOWER ENTERPRISE MOBILITY WITH MOBICONTROL

With over 10,000 enterprise deployments and millions of devices managed globally, SOTI's MobiControl is the world's most trusted Mobile Device Management (MDM) and Bring Your Own Device (BYOD) Management solution. MobiControl enables organizations to centrally manage, support, secure and track corporate-liable and employee-liable mobile devices, regardless of device type, mobile platform and location.

KEY BENEFITS:

Convenient Admin Control

Configure custom user groups and permissions for administrators to securely access the management web console anywhere anytime.

Secure Mobile Productivity

Manage access to the corporate sandbox on personal devices. Block access to unwanted features applications & games on corporate devices

Seamless Ease of Use

Enjoy the most intuitive business user interface to manage a variety of devices on multiple platforms in one solution.

Optimize Helpdesk Communication

Best-in-class remote support technology and live 2-way chat reduces call times..

Efficient Software Distribution

Custom application catalogs ensure all employees have secure and easy access to enterprise and 3rd party applications.

Mobile Inventory & Health Awareness

Track and report on a variety of live device information to monitor status, security, and condition of all mobile assets.